HIGH ASSURANCE DIGITAL SIGNATURES

ABSTRACT OF THE DISCLOSURE

A digital private key storage means containing a user's digital private key; a cryptographic engine; a communications port for receiving digital data from an external device, and for transmitting data to said external device; a display means for displaying said received digital data; a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data; wherein said cryptographic engine is trusted to only apply said user's digital private key to sign received data only if said user operable input means is operated, and to communicate said signed data external of said digital private key protection device. This arrangement secures the user's digital private key from end point attacks by trojan horse programs by virtue of the fact that the private key can only be accessed via the user operable input means which cannot be circumvented by software control.